DMSTTIAC

Defense Modeling, Simulation and Tactical Technology
Information Analysis Center

DMSTTIAC SOAR-99-03

Title: A Computer Modeling Challenge: Tracing Intelligence Data to SOF Mission Planning

19990604 228

A State-of-the-Art Report

John C. Chapman
Science Advisor
IIT Research Institute

Published by:
DMSTTIAC
IIT Research Institute
7501 South Memorial Parkway, Suite 104
Huntsville, Alabama 35802

April, 1999

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)

2. REPORT DATE
April 1999

3. REPORT TYPE AND DATES COVERED
State-of-the-Art-Review; April 1999

4. TITLE AND SUBTITLE
A Computer Modeling Challenge: Tracing Intelligence Data to SOF Mission Planning Systems

5. FUNDING NUMBERS

6. AUTHOR(S)
John C. Chapman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DMSTTIAC

8. PERFORMING ORGANIZATION REPORT NUMBER
DMSTTIAC SOAR 99-03

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
USSOCOM/SOIO-IN
Mission Support Branch
7701 Tampa Point Blvd
MacDill AFB, FL 33621-5323

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution authorized to Department of Defense and U.S. DoD contractors only. Other requests shall be referred to Commander Hq USSOOCOM/SOIO-IN, McDill AFB, FL 33621

12b. DISTRIBUTION CODE
"D"

13. ABSTRACT (*Maximum 200 words*)
Through years of intelligence architecture scrutiny and effort, one issue of interoperability continues to plague the intelligence community. Volumes of information have been produced on the capabilities of producing intelligence data and the operational uses for that data. Yet, no single source provides Intelligence planners and architects with clear traceability of data attributes to user requirements. Consequently, program managers for intelligence data/system enhancements have been constrained in their visibility into the operational impacts of intelligence program modifications. This report looks at current computer database/modeling efforts to assess the capability to produce a user-friendly model of the traceability between intelligence data and Special Operations mission planning systems.

14. SUBJECT TERMS
SOCOM, Intelligence, Mission Planning, Model, SOF, Special Operations

15. NUMBER OF PAGES
19

16. PRICE CODE
$70

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unclassified

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

A Computer Modeling Challenge: Tracing Intelligence Data to SOF Mission Planning Systems

A State-of-the-Art Review

John Chapman
Program Manager
IIT Research Institute

April 1999

TABLE OF CONTENTS

FIGURES

TABLE

A Computer Modeling Challenge: Tracing Intelligence Data to SOF Mission Planning Systems

1.0 BACKGROUND

The modeling of complex interrelationships between intelligence data and operational requirements has long been an objective of the Intelligence community. Architecture planning and analysis has been a formal program since the early 1980's. Its impetus was the Report on the National/Tactical Interface issued by the Secretary of Defense in 1978. Through various iterations it became known as the Command Intelligence Architecture/Planning Program (CIAP), which remained the program's name through May of 1996.

In 1996 the program changed emphasis. Actually, it broadened its focus as a result of the realignment of duties within the Office of the Secretary of Defense (OSD). The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) established, from other subordinate functions, the C4I Integration Support Activity (CISA). The CISA's challenge was to support ASD(C3I) and his/her deputies in assessing, developing, and integrating C4ISR requirements and systems. This resulted in redefining the CIAP program and its focus as the C4ISR* Integrated Architecture Program. In 1998 the CISA was dissolved as a Defense Support Activity and stewardship of the CIAP was transferred to the newly created Information Integration and Interoperability Directorate under the ASD(C3I). The next phase of evolution in this continuous process improvement effort is to further integrate C4ISR planning in a new Command Information Superiority Information Architecture (CISA) program. CISA's objective is to establish and sustain a responsive, interoperable, logical, and flexible plan for providing required C4ISR to the unified commands.[1]

Through all of this architecture scrutiny and effort, one issue of interoperability continues to plague the intelligence community. Volumes of information have been produced on the capabilities of producing intelligence data and the operational uses for that data. Yet, no single source provides Intelligence planners and architects with clear traceability of data attributes to user requirements. Consequently, program managers for intelligence data/system enhancements have been constrained in their visibility into the operational impacts of intelligence program modifications.

2.0 THE PROBLEM

The issue being investigated in this report is whether programs and/or technologies exist to provide dynamic modeling of the Intelligence-Operations data connectivity. (Note: the term Intel Data will be used in this report to represent all Intelligence, Surveillance, and Reconnaissance (ISR) data.) The following question was posed by representatives of USSOCOM/SOIO-IN: What is the current/planned capability in DoD to provide object-oriented (i.e., user-friendly) analysis of the effect that Intel Data modifications would have on Special Operations Forces (SOF) mission planning systems?

* C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

As an example, consider what could be the impact of eliminating 100-meter digital terrain elevation data (DTED) in favor of data at 10-meters or less. If current capabilities made this approach feasible, and the Intelligence community decided to "improve" their service in this way, would there be a user somewhere whose system could no longer receive or use the data? The USSOCOM dilemma is exacerbated by their reliance on all Services' and other government agencies' intelligence support, over which they have little direct influence. Data connectivity visibility is not a SOF-only problem; it has direct applicability to all Services and unified commands.

Consider also the situation which occurred as the Air Force Mission Support System (AFMSS) was being developed. Early planning identified automated interfaces with the Consolidated Intelligence Database (CIDB). AFMSS uses Portable Flight Planning Software (PFPS) to perform route-of-flight calculations. PFPS is used by SOF component (USAF/USN) forces, providing route planning and communication data and automated updates to aircraft systems. The PFPS uses Intel Data such as DTED, mapping data from the National Imagery and Mapping Agency (NIMA), and threat order of battle information.

Concurrent with the PFPS development, Intelligence began development of their Modernized Integrated Database (MIDB). When PFPS was ready to interface the requisite Intel Data for SOF applications, the data (MIDB) could not be read by the PFPS software. The MIDB program management had no prior indications of this potential problem. When the software development engineers were queried, they soon identified the cause: the Intel Data had changed format and was incompatible with PFPS. This was a fundamental disconnect in coordinating requirements.[2]

Requirements definition and coordination difficulties present the greatest challenge to program managers. Numerous Integrated Product/Process Teams (IPTs) and dedicated manpower are generally required in order to attempt to avoid such disconnects. The data interconnectivity model sought by the USSOCOM/SOIO-IN staff would help correct that problem with an easy-to-use analysis tool to survey user impacts prior to implementing Intel Data changes.

3.0 MODEL CONSIDERATIONS

To better understand the modeling effort that is required, we need to first look at the type of representation and level of detail necessary to produce the desired results. This requires an assessment of the architecture view and data elements required for representation in the model.

3.1 ARCHITECTURES

The modeling of data interchange functionality begins with a representation of the architecture in which it operates. To avoid confusion, the term "architecture" needs to be defined. The term architecture has a variety of meanings depending upon the context in

which it is being used. In C4ISR and other architecture modeling efforts, the purpose for the model's use determines the model's scope and architecture category. The DoD C4ISR Framework[3] document provides the definitions below for three different categories of architectures: operational, systems, and technical.

a. Operational Architecture: A description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation.

b. Systems Architecture: A description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions.

c. Technical Architecture: A description of the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Each architecture views the interactions of systems and functions with a different perspective. However, each view also addresses some of the same functional descriptions as the others, since the real world functions don't operate in one view only. Based on the modeling problem and objective posed by USSOCOM/SOIO-IN, a detailed architecture picture is needed to analyze the interconnectivity between Intel Data and automated Operations mission planning. While an operational-level review is required in order to identify essential Information Exchange Requirements (IERs), the details for traceablility will come primarily from a systems architecture view. As the C4ISR Framework document points out, this systems-level view will include

a. Identifying systems interfaces and defining the connectivities between them,

b. Defining system constraints and their bounds of performance behavior, and

c. Identifying technological interdependence, showing how multiple systems link and interoperate, including the internal operation of particular systems.[3]

3.2 MISSION PLANNING REQUIREMENTS

Requirements for Intel Data are driven by operational needs. In this report, the focus is on data required for mission planning systems used to support SOF missions. Each of the Service components has mission planning software in various stages of development/implementation. While most Intel Data is currently input into these systems manually, continuous improvements of applications such as the PFPS, as well as integrated mission planning systems, make Intel Data traceability more critical as time goes on. One such example is the Naval Special Warfare (NSW) Automated Mission Planning System (SWAMPS).

The SWAMPS program is developing a laptop-based capability to provide NSW tactical mission planners with automated planning/assessment tools. These tools will provide threat, meteorological/oceanographic (METOC), and other mission planning-related databases; and access to facilitate effective and timely mission planning. SWAMPS will include an automated Mission Planning Guide, drawing tools, message parsing and

generation, and connectivity to the NSW Tactical Aircraft Mission Planning System (TAMPS). TAMPS will provide route planning, maps/charts, plus database and communications interfaces. Intel Data requirements for SWAMPS include the following:

a. DTED
b. METOC
c. Imagery
d. Naval Order of Battle (NOB)
e. Enemy mining
f. Littoral threats
g. Target data--location, orientation, construction, etc.

Another planning system, called Joint Special Operations Forces Mission Planner (JSOMP), is currently under development by USSOCOM/SOAL (Fig. 1). Prototype JSOMP functionality has been demonstrated in Southwest Asia in actual operations with CENTCOM's Special Operations Command (SOCCENT) staff. JSOMP provides a PC-based decision support tool to Joint Special Operations Task Force (JSOTF) and Special Operations Component (SOC) commanders. It integrates the Service Components' mission planning software into a system with interfaces for common supporting data, including Intel Data. SOCCENT has found the capability especially useful in planning various courses of action and briefing them to decision-makers. A representation of the total JSOMP system is depicted below, with generic interfaces to support component Automated Mission Planning Systems (AMPS).

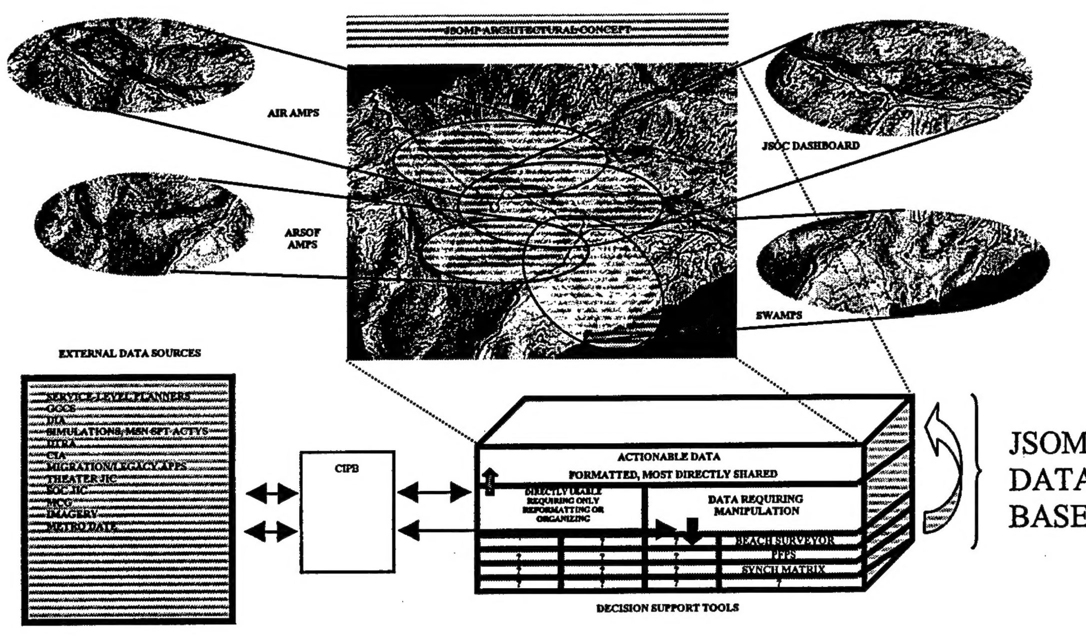

Figure 1. JSOMP Functional Representation (OPR: USSOCOM/SOAL/PEO-IIS-C4IAS)

The key elements of this representation that reflect Intel Data exchange are the External Data Sources and the Collaborative Intelligence Preparation of the Battlespace (CIPB),

which provide the requisite input data to this JSOMP system. This utilizes and builds on the same approach successfully implemented by SWAMPS, i.e., using the CIPB to consolidate and distribute the Intel Data to remote mission planning systems. Specific JSOMP data requirements include those identified above for SWAMPS, plus additional data for the other supported planning systems:

a. Ground Order of Battle (GOB)
b. Air Order of Battle (AOB)
c. Electronic Order of Battle (EOB)
d. Threat Data--Locations, Ranges, Frequencies

3.3 INTELLIGENCE DATA

The resulting demand on ISR systems to produce and deliver Intel Data has created large data sets and delivery options available to potential users. In relation to the specific requirements for SOF mission planning systems, as indicated above, a wide variety of data element attributes is available. The table below shows only a small subset of the types of data that the Intelligence community has continued to improve over the years in order to meet their operational customers' needs. It is these types of data elements, and the host of other "INT" (COMINT, ELINT, etc.) data not represented , which Intelligence is seeking to model for improved visibility into the impact of system "enhancements". Such a model would go a long way toward solving the problem of requirements disconnects during product/process improvement efforts.

INTELLIGENCE DATA

TYPE	MODES	DATA/INFORMATION
IMINT	Radar EO IR	Position Elevation Orientation Vegetation Target Characteristics Enemy Locations Defenses
SIGINT	Aircrew UAV Satellite Ground	Frequencies EOB Signature Operating Mode - Acquisition - Target Tracking - Fire Control

Table 1. Representative Intelligence Data

Intelligence systems and processes continue to be enhanced in order to meet the operational customers' needs for data collection, evaluation, and distribution. As noted in the example above, intelligence database information has been evolving to take advantage of technology enhancements, and to better meet the needs of the warfighter. Over the last several years, the CIDB has changed through several iterations to become its current version of the MIDB. The MIDB continues to undergo an evolutionary development. Initial emphasis is on the integration of separate intelligence databases into a single, relational structure for enhanced functionality.

Given the increasing complexity of relationships between Intelligence functions and operational users, the traceability of data has become unresponsive to the needs of intelligence systems managers, in seeking to achieve program efficiencies and enhancements. Technology and operational necessity have driven the system to such a complex global network of data sharing (Fig. 2) that the reliability of manual identification of impacts to change has become extremely problematic.

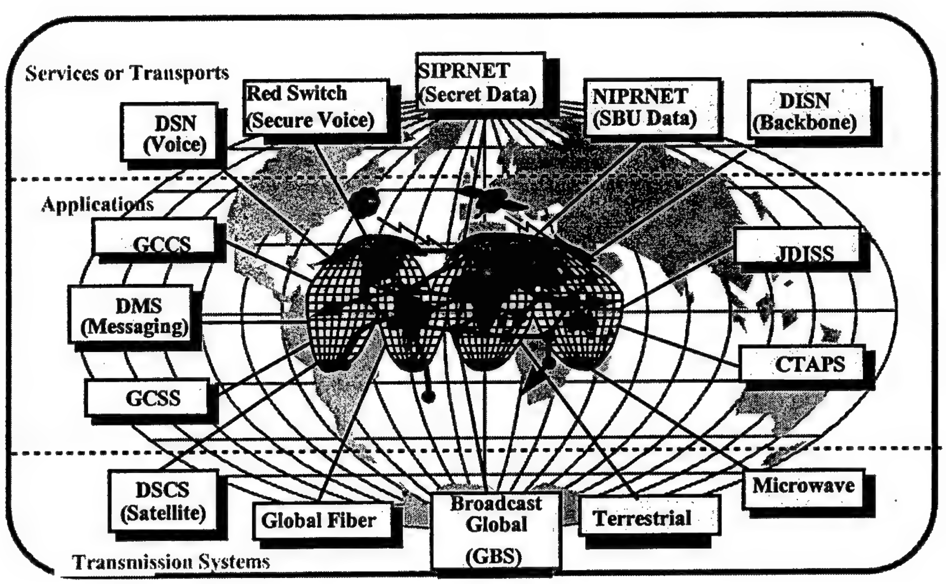

Figure 2. Global Networked Information Enterprise (GNIE), Defense Information Infrastructure (OPR: Joint Staff/J6)

This results in after-the-fact efforts to fix disconnects, such as in the PFPS-MIDB example noted above. To avoid such disconnects, programs must invest in significant data searches and IPT activities in order to identify all affected users, systems, and equipment--with no set of tools to ensure that all potential impacts are accounted for. The effective use of computer models to analyze such complex relationships is, however, being proven in numerous applications across DoD.

4.0 CURRENT MODELS

The Intel Data modeling challenge is not unique, though its application is. Therefore, we should first look at some of the existing programs which model, to varying degrees, the connectivity of Intel Data to operational systems. No current programs, however, focus on the specific data traceability challenge posed by the Intelligence community. The three modeling efforts noted below illustrate the emphasis within DoD being placed on using robust data representations to analyze the capabilities of information systems and force structure. These efforts demonstrate various levels of detail, based upon their specific application, and each shows potential to address the Intel Data traceability challenge.

4.1 Joint Mission Analysis (JMA)

In USSOCOM the Strategic Planning Process (SPP) uses a JMA database to assess the resource requirements for SOF missions (Fig. 3). Mission profiles are planned for the full range of potential SOF missions, as dictated by scenarios that support the Defense Planning Guidance. This results in approximately 24,000 combinations of SOF forces, equipment, and tactics to meet the specific mission objectives required by the various illustrative planning scenarios.[4]

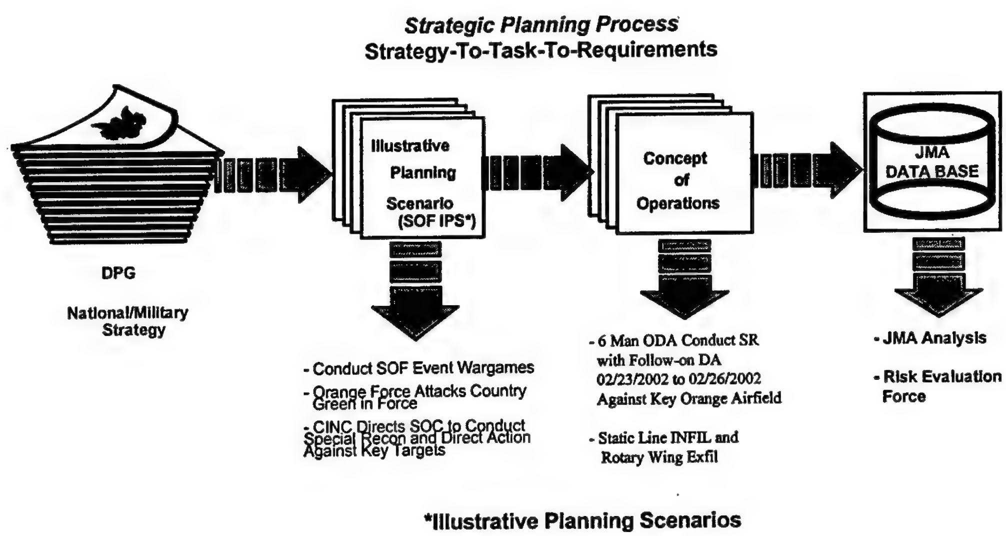

Figure 3. USSOCOM Strategic Planning Process

Current modeling of these capabilities provides the capability to display graphical representations of units and the C4ISR connectivity to them. The JMA database provides sufficient detail to analyze and to display the time-phased impacts of primary mission

functions, such as the preparation phase, infil, action on the objective, exfil, and recovery. Supported by the SOF Analytical Modeling System (SOFAMS), the JMA process can produce visual representations of mission deployment data and timelines (Fig. 4).[5]

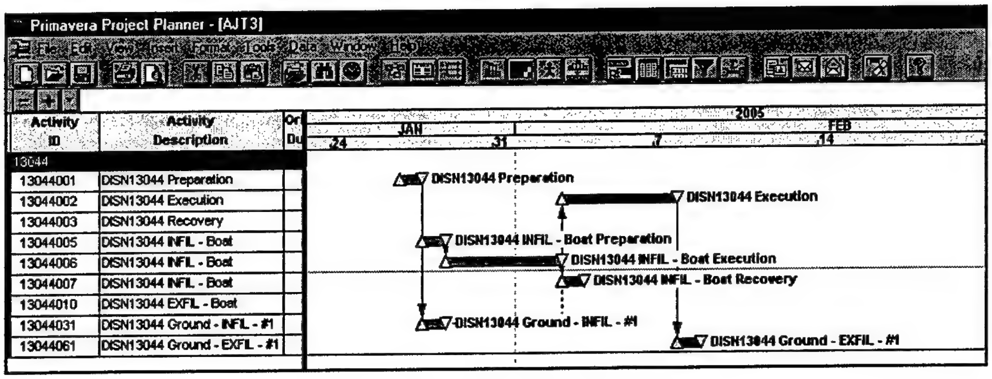

Figure 4. SOFAMS Time Analysis

The problem that remains, however, is the absence of sufficient data detail to assist Intelligence planners in their quest to clearly link Intel Data requirements to operators' data applications in these graphical representations. The missing level of detail includes the specific data and equipment requirements for mission preparation/rehearsal and for mission execution, where unique support may be necessary. This unique support could be, for example, in the form of direct intelligence feeds to and from deployed teams, i.e., electronics (ELINT), signals (SIGINT), human (HUMINT), or other types of intelligence information. This is not captured in the JMA database. The reason, however, is simple: the SPP, which the JMA is designed to support, does not require it. The JMA process is specifically designed to determine unit and platform requirements in a relatively unconstrained simulated application of SOF capabilities in illustrative planning scenarios. This force sizing is then modified to an objective force by USSOCOM's Assessment Directors based on obtaining operational efficiencies and assuming reasonable levels of risk. The modeling of detailed data/information exchange requirements is not the objective of JMA.

4.2 Joint C4ISR Architecture Planning/Analysis System (JCAPS)

In support of the CIAP program, soon to be CISA, analytic tools are being developed under the JCAPS program. JCAPS is being designed to provide a common Command/Service/Agency networked architecture information display, integration and analysis capability. JCAPS is a validated requirement for C4 systems, as approved by the Global Command and Control System (GCCS) Requirements Board on 13 Nov 97. The GCCS functionality, as depicted below (Figure 5), will be simulated by JCAPS to provide graphical support to analysis and development of C4 architectures. The JCAPS database support employs the same Shared Database Environment (SHADE) concept as GCCS for owner-controlled data protection and sharing. It replicates GCCS universal

and shared data, incorporates security features for eventual multi-level security operations, and enables site-to-site collaborative development of architectures.

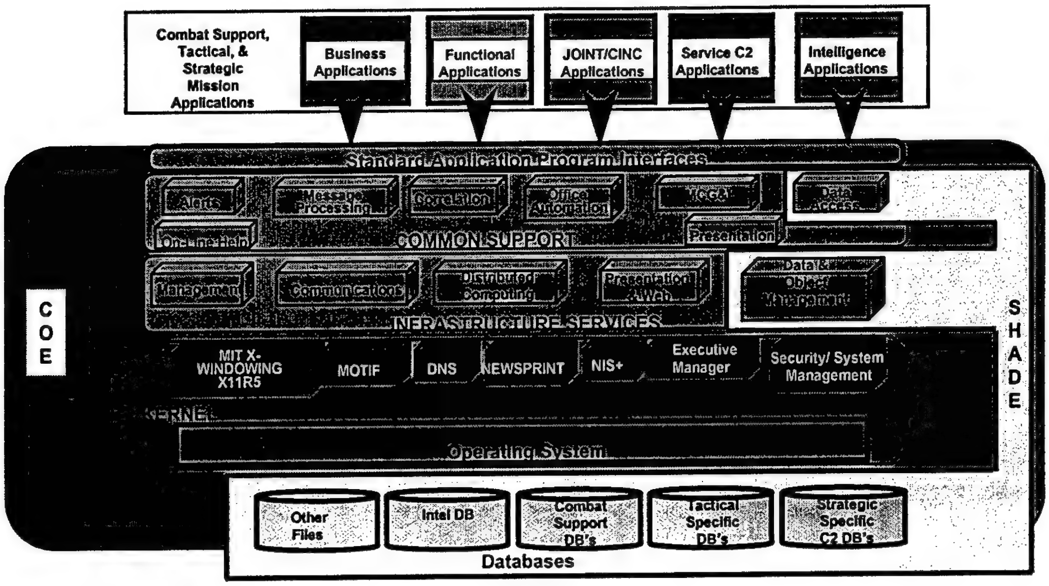

Figure 5. Global Command and Control System (GCCS)

The graphic below (Fig. 6)[6] displays two of the views being incorporated into the initial C4 applications of JCAPS. They represent a functionality that could also be expanded or adapted to provide Intelligence planners with the analytic tools necessary to link Intelligence and Operations data requirements.

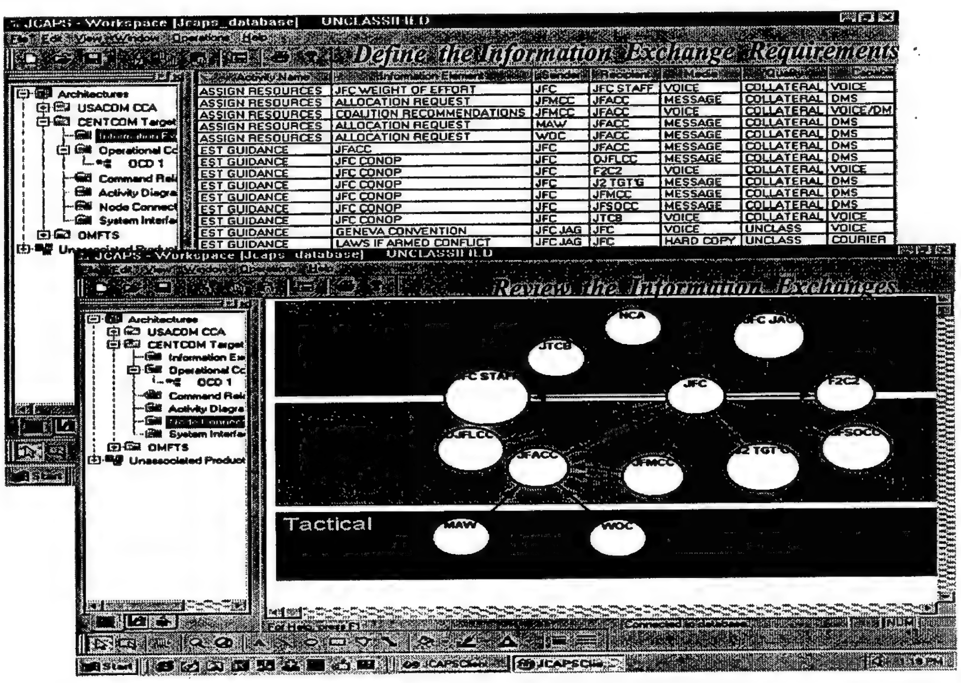

Figure 6. JCAPS User Views

The JCAPS plan is to include ISR systems' functionality in JCAPS as a planned improvement. The current plan for JCAPS, however, (Fig. 7)[6] will not deliver such capability until all higher level functionality is achieved.

Version 1	Version 2	Version 3	Version 4
• Arch Fmk V2 Products • Web-Based Browser • Baseline Database • SIM Functionality • Limited Analytical Capabilities • Cross-Arch Analysis Capability • Network Loading/Performance Analysis • Initial Arch Modeling and Simulation Spt	• CIAP Documentation • Complete AF V2 Products • Mapping • Node-to-Node Replication • DII COE Level 6 • Interoperability Assessment • Interactive Database Support • PPBS Support • Transition Planning	• Threat Assessment • "What if" Capabilities • Performance Measurements • Metrics • Enhanced M&S Support	• Cost-Benefit Analysis • Enhanced MOEs • Multilevel Security
Jun - Nov 98	Oct 99	Oct 00	Oct 01

Figure 7. JCAPS Schedule

One JCAPS modeling effort that offers significant promise for modeling Intelligence-Operations data exchanges is the Network Warfare Simulation (NETWARS). NETWARS is being developed to perform detailed modeling of tactical communications systems across the Services. It will also provide linkage to the Joint Warfare Simulation (JWARS) for joint analyses and to the Joint Simulation System (JSIMS) for joint training, as well as to JCAPS. NETWARS is specifically designed to capture and display the dynamics of communications infrastructure and information exchanges. The level of detail available to characterize communications networks, nodes, equipment, and transmission characteristics, could be readily adapted to the analysis of Intel Data. As the timeline below (Figure 8) shows, NETWARS is planned to evolve into a robust analytical tool.[6]

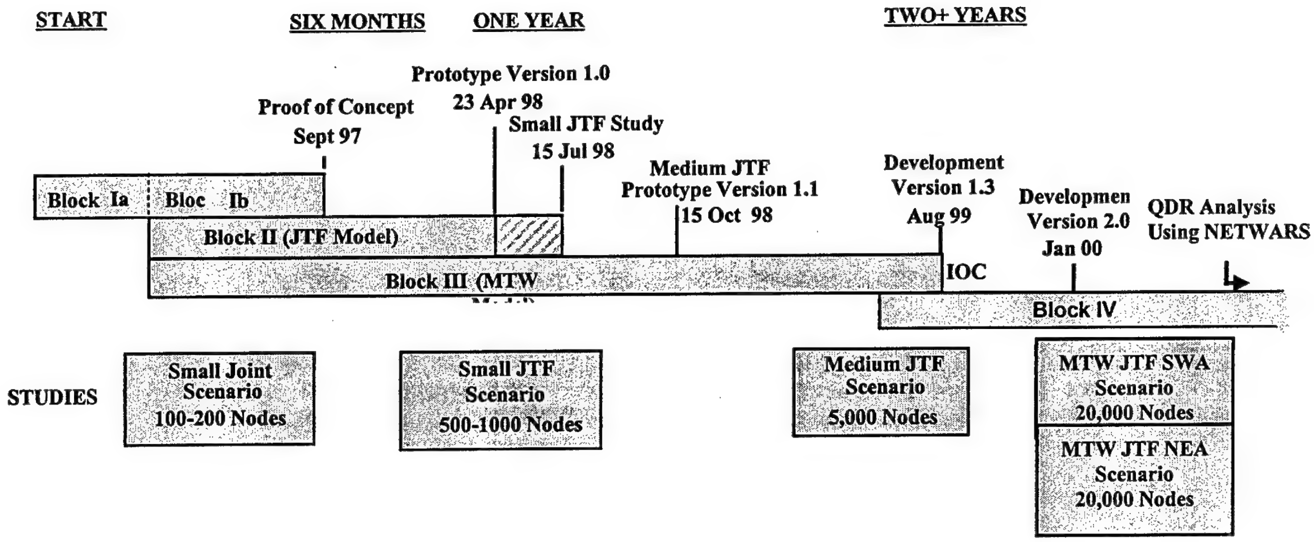

Figure 8. NETWARS Development (OPR: Joint Staff/J6I)

4.3 General Campaign Analysis Model (GCAM)

This modeling challenge is being worked by other DoD agencies as well. The Navy has been developing the GCAM to assist in analysis efforts to support their own Joint Mission Analysis, as well as their Investment Balance Review (IBR) and Quadrennial Review (QDR) processes. GCAM provides a flexible tool set for modeling from the joint campaign to the engagement level. Ongoing development is sponsored by CNO/N81 based on guidance from the Joint Analytic Model Improvement Program (JAMIP). Similar to the USSOCOM JMA/SOFAMS process, the Navy's use of GCAM provides a detailed assessment of capabilities to support force sizing (Figure 9).

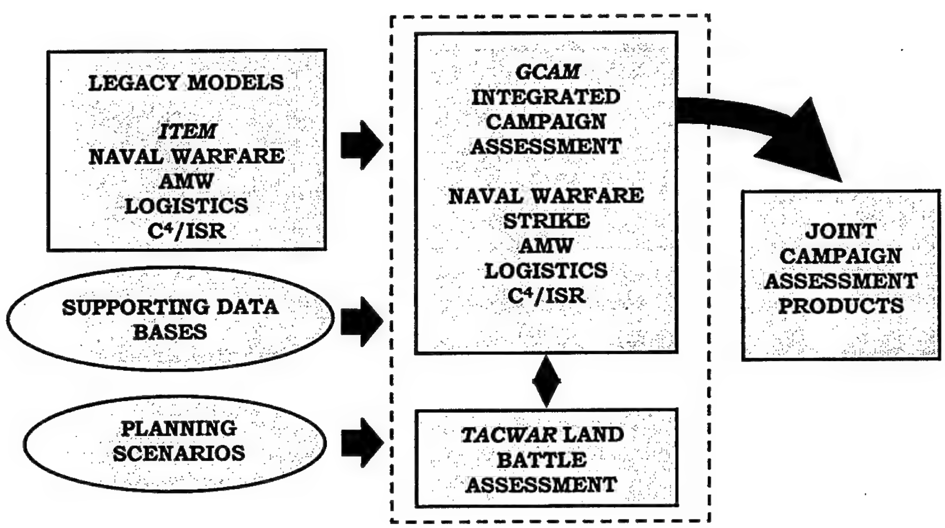

Figure 9. DON PR-99 Analysis and N-81 QDR Process

GCAM is an object-oriented model designed to provide analyst-defined unit interfaces in a common mapping environment for joint campaign analysis. Unlike USSOCOM's JMA, GCAM has developed to the point of accounting for damage and attrition in the scenarios. Tradeoff analyses account for cross-mission, cross-platform alternative force structure solutions. Results can be obtained to display force application alternatives such as the ones in the example below (Figure 10).

Type Run	Description	Kills Before Red Launch	Total Acquisitions	P_{ACO}	P_K
Baseline	Baseline	653 of 6000	1740 of 6000	0.29	0.28
Variant A	One Surveil A/C	62% less	56% less	0.13	0.12
Variant B	Deck Launch TACAIR	84% less	10% less	0.26	0.25
Variant C	Better Surveil Sensors (x2)	54% more	47% more	0.43	0.41
Variant D	Double Red Transit Time	33% more	41% more	0.41	0.39

Variants shows changes in P_{ACQ}, total acquisitions and kills before launch for different run conditions

Figure 10. GCAM C4ISR Baseline vs. Variants

GCAM provides a flexible approach to modeling that enables analysis of warfighting and support capabilities from joint campaign to engagement levels. The Navy is continuing to develop GCAM with an eye toward potential applications such as the following:

a. Warfighting assessments
   1. End-to-end campaign assessment
   2. Cost-effectiveness analysis

b. Wargaming support
   1. Implement tactics
   2. Support decision-making
   3. Evaluate new warfighting technologies

c. Training support
   1. CONOP development
   2. Flexible Deterrent Options (FDO) testing
   3. Force Sequencing.

The level of resolution, the amount of supporting data integration and the scope of GCAM application cases is variable and depends on the requirements of individual analysis efforts. GCAM also provides dynamic graphical display during application execution as well as graphical output and results summaries. A program called

ObjectManager provides editors, map-based tools, object templates, and network display tools for viewing and editing command and reporting architectures and object structures.[7]

5.0 Model Design Criteria

To use modeling and simulation in the joint environment (USSOCOM's only environment), certain DoD/joint standards and integration activities must be accommodated. Current and developmental joint models are addressing conformance or compliance, as appropriate, in their program plans. Any potential Intel Data model would necessarily address these evolving joint standards. Three key programs are fundamental in assessing/developing a joint intelligence database traceablility model.

5.1 Year 2000 (Y2K)

This government-mandated program is designed to ensure that computer operations and software applications are not adversely impacted by their date data when the year 2000 starts. All government architectures and applications have been required to assess and correct potential discrepancies. This is a complex issue and some systems/programs have had more difficulty than others in achieving Y2K compliance.

JMA/SOFAMS represents a new and evolving software implementation of the USSOCOM Strategic Planning Process and is being designed and delivered Y2K compliant. Y2K compliance is not expected to be a problem as the system is already operating in the 2007 planning year.

JCAPS/NETWARS, as a relatively new development effort, has been constructed from its inception to be Y2K compliant.

GCAM/ObjectManager is also Y2K compliant and, like JMA, also dealing with analysis of warfighting and support capabilities addressing years beyond 2000.

5.2 High Level Architecture (HLA)

The HLA is a DoD program to promote simulation reuse and interoperability. Its fundamental approach is to provide a simulation architecture foundation that supports and enhances interaction among various simulations. The intent is to encourage simulation owners and users to develop a variety of applications for their simulations. The objective is to reduce time and cost in producing simulations, through the use of multiple, flexible, and collaborative applications of individual simulations.

HLA is mandated for DoD simulations and models interactivity. The Undersecretary of Defense for Acquisition and Technology policy states, "The Department shall cease further development or modification of all simulations which have not achieved, or are not in the process of achieving, HLA compliance by the first day of FY 1999, and shall retire any non-compliant simulations by the first day of FY 2001."[8]

JMA/SOFAMS has not addressed HLA compliance. It does not represent nor support any simulation system at this time. SOFAMS input and analysis software used to build the JMA database are internal, stand-alone systems. The JMA database is an Oracle relational database and supports data export in varying formats as needed. As a potential foundation to the Intel Data traceability model, JMA/SOFAMS would need to be adapted for HLA compliance to accommodate any data exchange interactions with joint models.

JCAPS/NETWARS compliance with HLA standards is being accommodated through its use of a commercial communication network simulation model called Operating Network Engineering Tools (OPNET). OPNET is part of a Defense Advanced Research Projects Agency (DARPA) project creating a federation of simulations that will exercise the HLA standards and interface tools. As a result, the JCAPS/NETWARS will provide extended capability for future applications of their development efforts.

GCAM/ObjectManager has been funded and programmed to become HLA compliant by the end of FY99.

5.3 Defense Information Infrastructure (DII) Common Operating Environment (COE)

The Defense Information Infrastructure (DII) Common Operating Environment (COE) is an ASD (C3I)-mandated program to ensure timely, accurate information flow to the warrior. It will provide information software integration and interoperability among DoD offices, agencies, and commands. It identifies reusable software components and a software infrastructure for supporting mission-area applications, guidelines, standards, and specifications. The Services, Agencies, and other DoD Components are responsible for DII COE compliance (including the enforcement, budgeting, and scheduling). GCCS relies heavily on the DII COE to promote interoperability through sharing common communications, applications and information.[9]

The DII COE Integration and Runtime Specification (I&RTS) outlines the guidelines and rules for implementation. It describes how to reuse existing software and properly build new software so that integration is seamless, and, to a large extent, automated. The DII COE defines eight progressively deeper levels of integration for the runtime environment. These levels are directly tied to the degree of interoperability achieved. The I&RTS document is the result of the collaboration among the Services, Joint Staff, USD(A&T), ASD(C3I), DISA, DIA and other elements of the Intelligence Community.[10]

JMA/SOFAMS is built with standard, off-the-shelf geospatial information, database, and project planning systems linked by Visual Basic code. It is run under Windows NT (user PC station) and Sun Solaris (database Sun server) over the USSOCOM classified LAN. No other systems are integrated with it, though reusability of modules is high given the standard software used for implementation. DII COE compliance would be achievable, based on the standard system capabilities, but is not addressed at this time.

JCAPS/NETWARS applications have no current requirement for DII COE compliance. The basic JCAPS application has been developed to be Level-5 compliant, though verification testing has yet to be accomplished. The additional simulation capabilities of NETWARS, however, have not incorporated DII COE requirements, though they have been designed with future adaptation in mind. Since future GCCS applications will have need for the C4ISR data being support by the JCAPS/NETWARS program, DII COE will eventually become an issue.

GCAM/ObjectManager is not currently addressing DII COE standards in its development. As a Navy analysis tool, it has been used largely in closed environments where information portability and interoperability are not issues. The current use of GCAM to provide scenario analyses does not require any remote data linkage or distributed processing. However, Visual Basic and standard software tools are used to produce Windows NT applications which will be adaptable to DII COE as required.

6.0 Summary

The above three examples of capabilities assessment modeling show that significant effort is being expended to capture, analyze, and display information for decision-makers. With respect to the Intel Data traceability challenge facing the intelligence community, there is no known modeling program dedicated toward that end.

USSOCOM's JMA/SOFAMS program has developed an extensive database of SOF operational capabilities. Intelligence functions are modeled at a nodal level of detail. Adding the requisite additional levels of detail to achieve the data traceability objectives sought by USSOCOM SOIO/IN planners would be a significant, but achievable task. Nonetheless, the JMA database represents an important foundation upon which to build the proposed Intel Data model. Such an undertaking would necessarily require accurate and current representations of SOF force structure and employment options, and the JMA provides that data.

The ASD(C3I)-directed C4ISR architecture development efforts (CIAP and its predecessors) have created detailed, standardized data requirements that allow common representations of capabilities across DoD. The JCAPS/NETWARS program is producing usable information to define and assess C4ISR architectures. The shortfall is in the usability of the information for CINCs' staffs. The type of forward-thinking "what if" questions being asked by the SOIO/IN staff can not be answered by the current or planned JCAPS automated tools.

The GCAM/ObjectManager program is only one example of other organizations' efforts to use automated data analysis to answer capabilities assessments. It shows the detail that can be achieved in comparing the effect of various excursions on combinations of resources applied to given operational scenarios. The same type of comparative analysis is exactly what the SOIO/IN planners are seeking, with the specific application of representing detailed Intel Data coupled to mission planning systems, or other Operations applications.

7.0 Recommendation

The Intel Data traceability task postulated by USSOCOM/SOIO-IN planners is achievable. Modeling efforts discussed in this report could each be adapted and expanded to create the desired results. However, none of the programs discussed have an Intel Data modeling charter. Tailored applications, along with the additional requisite data detail, will be required in order to provide the capability.

Recognizing that a technological solution is feasible, the first step would be a more detailed study of government and commercial modeling and display efforts to identify the most effective solution for Intelligence. The solution must provide maximum flexibility to address joint data interchanges and, therefore, must meet all DoD interface standards, such as HLA and DII COE.

Once an approach is chosen, database development, adaptations and interfaces would be identified. The application could then be tailored to provide responsive, graphical representations of the information required. This tool would assist Intelligence planners in analyzing potential Intelligence-Operations data disconnects and identifying efficiencies that should be pursued.

REFERENCES

1. Draft Statement of Work for Command Information Superiority Architectures (CISA), 29 October 1998.

2. Interview with 1Lt Cade Anderson, USSOCOM/SOIO-IN-JIC

3. C4ISR Architecture Framework, Version 2.0, 18 December 1997.

4. USSOCOM Directive 1-9, 22 May 1997

5. JMA Briefing, OPR: USSOCOM/SORR-SCA

6. JCAPS briefing, "Unraveling the Architecture Knot", OPR: JCAPS PM, OASD(C3I)/II&I

7. General Campaign Analysis Model, Version 2.3, Navy Modeling and Simulation Information System Catalogue (http://navmsmo.hq.navy.mil/nmsiscat)

8. USD(A&T) Memorandum, "DoD High Level Architecture (HLA) for Simulations," 10 September 1996.

9. ASD (C3I) Memorandum, "Implementation of Defense Information Infrastructure Common Operating Environment Compliance, " 23 May 1997.

10. DII COE Integration and Runtime Specification (I&RTS), CM-400-01-03, 1 January 1997.

GLOSSARY

AFMSS	Air Force Mission Support System
AOB	Air Order of Battle
ASD	Assistant Secretary of Defense
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIA	Central Intelligence Agency
CIAP	Consolidated Intelligence Architecture Program; C4ISR Integrated Architecture Program
CIDB	Consolidated Intelligence Database
CINC	Commander in Chief (of Unified Commands)
CIPB	Collaborative Intelligence Preparation of the Battlespace
CISA	C4I Integration Support Agency; Command Information Superiority Architecture
COE	Common Operating Environment
COMINT	Communications Intelligence
CONOP	Concept of Operations
CTAPS	Contingency Theater Automated Planning System
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISN	Defense Information System Network
DMS	Defense Message System
DSN	Defense Switched Network
DSCS	Defense Satellite Communication System
DTED	Digital Terrain Elevation Data
ELINT	Electronic Intelligence
EOB	Electronic Order of Battle
FDO	Flexible Deterrent Option
GBS	Global Broadcast System
GCAM	General Campaign Analysis Model (Navy)
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GOB	Ground Order of Battle
HUMINT	Human Intelligence
I&RTS	Integration and Runtime Specification (for DII COE)
IBR	Investment Balance Review (Navy)
IPT	Integrated Product/Process Teams
JAMIP	Joint Analytic Model Improvement Program
JCAPS	Joint C4ISR Architecture Planning/Analysis System
JDISS	Joint Deployable Intelligence Support System
JIC	Joint Intelligence Center

JMA	Joint Mission Analysis
JSIMS	Joint Simulation System
JSOMP	Joint Special Operations Mission Planner
JWARS	Joint Warfare Simulation
LAN	Local Area Network
MCG	Mapping, Charting and Geodesy
MIDB	Modernized Integrated Database
NETWARS	Network Warfare Simulation
NIPRNET	Nonsecure Internet Protocol Router Network
NOB	Naval Order of Battle
OPNET	Operating Network Engineering Tools
PFPS	Portable Flight Planning Software
QDR	Quadrennial Defense Review
SHADE	Shared Database Environment
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SOFAMS	Special Operations Forces Analytic Modeling System
SPP	Strategic Planning Process
SWAMPS	Special Warfare Automated Mission Planning System (Navy)
Y2K	Year 2000